

OTIMIZANDO TÉCNICAS DE HARDENING COM INTELIGÊNCIA ARTIFICIAL

OPTIMIZING HARDENING TECHNIQUES WITH ARTIFICIAL INTELLIGENCE

Evandro Ferreira Melo Pires, Faculdade de Tecnologia de Araraquara
evandro.pires@fatec.sp.gov.br

João Emmanuel D' Alkmin Neves, Faculdade de Tecnologia de Araraquara
joao.neves11@fatec.sp.gov.br

Resumo

O presente artigo aborda o uso de inteligência artificial como uma ferramenta complementar à consulta de livros no gerenciamento e configuração de servidores para fortalecimento do hardening, que é um termo utilizado para descrever os processos de proteção de um sistema, na intenção da redução de possíveis vulnerabilidades. Embora os livros ofereçam informações confiáveis, a IA fornece respostas instantâneas, apesar que nem sempre com a mesma qualidade. O problema abordado é a necessidade de obter informações sobre segurança cibernética de forma rápida e eficiente, pois os livros demandam tempo para pesquisa e leitura. A hipótese é que a IA pode agilizar e auxiliar na compreensão e implementação de boas práticas de Segurança da Informação. Os objetivos são destacar a evolução tecnológica e a utilidade do chatbot desenvolvido pela OpenAI baseado na arquitetura GPT (Generative Pre-trained Transformer), além de ressaltar suas vantagens e limitações em comparação com a consulta de livros. A justificativa está na importância crescente da segurança cibernética e na necessidade de ferramentas eficientes para auxiliar os profissionais nessa área.

Palavras-chave: Segurança Cibernética, Inteligência Artificial, Evolução Tecnológica.

Abstract

This article discusses the use of artificial intelligence as a complementary tool to consulting books in server management and configuration to strengthen hardening, which is a term used to describe the processes of protecting a system with the intention of reducing possible vulnerabilities. Although books provide reliable information, AI provides instant answers, although not always with the same quality. The problem addressed is the need to obtain information on cyber security quickly and efficiently, as books require time to research and read. The hypothesis is that AI can speed up and help in the understanding and implementation of good Information Security practices. The objectives are to highlight the technological evolution and usefulness of the chatbot developed by OpenAI based on the GPT (Generative Pre-trained Transformer) architecture, as well as highlighting its advantages and limitations compared to consulting books. The justification lies in the growing importance of cyber security and the need for efficient tools to help professionals in this area.

Keywords: Cybersecurity, Artificial Intelligence, Technological Evolution.

1. Introdução

A Evolução é um fenômeno que traz consigo percepções positivas e negativas, dependendo muito de suas aplicações, que geralmente geram incertezas e expectativas. As experiências ao longo do tempo envolveram importantes descobertas de grandes estudiosos, como Marie Curie, que complementou a descoberta do elemento chamado rádio e dos raios-x. Essas descobertas tornaram-se assuntos muito discutidos. Inicialmente, acreditava-se que a radiação do rádio poderia ter efeitos terapêuticos em doenças como o câncer, e a indústria incorporava o rádio em seus produtos, como tônicos revigorantes e até mesmo chocolates radioativos. A partir dessas observações, é possível perceber que a evolução proporciona desafios que exigem pesquisa contínua em busca de respostas autênticas.

E hoje em dia, sem essas descobertas, muitas das aplicações existentes não seriam possíveis. Tendo como base esse contexto, refletir sobre a evolução que se vive atualmente. Em que fala muito sobre o Generative Pre-trained Transformer Chat, ou Chat transformador pré-treinado generativo, comumente conhecido como Chat GPT, desenvolvido pela OpenAI. Diariamente são identificadas inúmeras aplicações, que podem ter perspectivas positivas e negativas. No caso deste estudo, que tem como propósito explorar os benefícios trazidos pela evolução dessa ferramenta, busca-se aproveitar sua capacidade de proporcionar pesquisas mais rápidas em comparação com a utilização de livros, os quais possuem informações mais detalhadas e demandam mais tempo e esforço para serem compreendidos, a intenção é utilizar como um norteador de problemas ou soluções que possam servir de apoio aos livros, para potencialização das técnicas do gerenciamento e configuração do hardening em servidores, com foco na segurança das informações.

A expressão hardening na língua inglesa se refere a “endurecimento”, que também é utilizado para descrever os processos de proteção de um sistema, na intenção da redução de possíveis vulnerabilidades, pode ser considerado o “fortalecimento” do sistema. Os recursos que apoia essa ideia são as configurações preventivas que podem ter variações, como diversas configurações, instalação de pacotes de segurança e permissões.

2. Referencial Teórico

De acordo com Melo (2014, p.3) sistemas operacionais modernos incorporam várias medidas de controle para aprimorar a segurança e otimizar a utilização dos recursos. No entanto, quando

se trata de um sistema operacional moderno projetado para fornecer serviços de rede, é correto que esses controles estejam desativados. Pode ser evidenciado pelo fato de que a maioria das distribuições é suscetível a um ataque conhecido como “fork bomb”, que consiste em esgotar os recursos do sistema, abrindo repetidamente processos até que não haja mais recursos disponíveis e o servidor seja travado.

Com inovações das tecnologias atuais e que estão em constante evolução, alguns pensam neste fenômeno virá causar muitos problemas, como acabar com alguns tipos de empregos ou afetar a segurança cibernética, por outro lado tem a positividade, que pode se aproveitar essas condições para favorecer a ampliação do conhecimento aliadas aos padrões já existentes, como pesquisas nos livros.

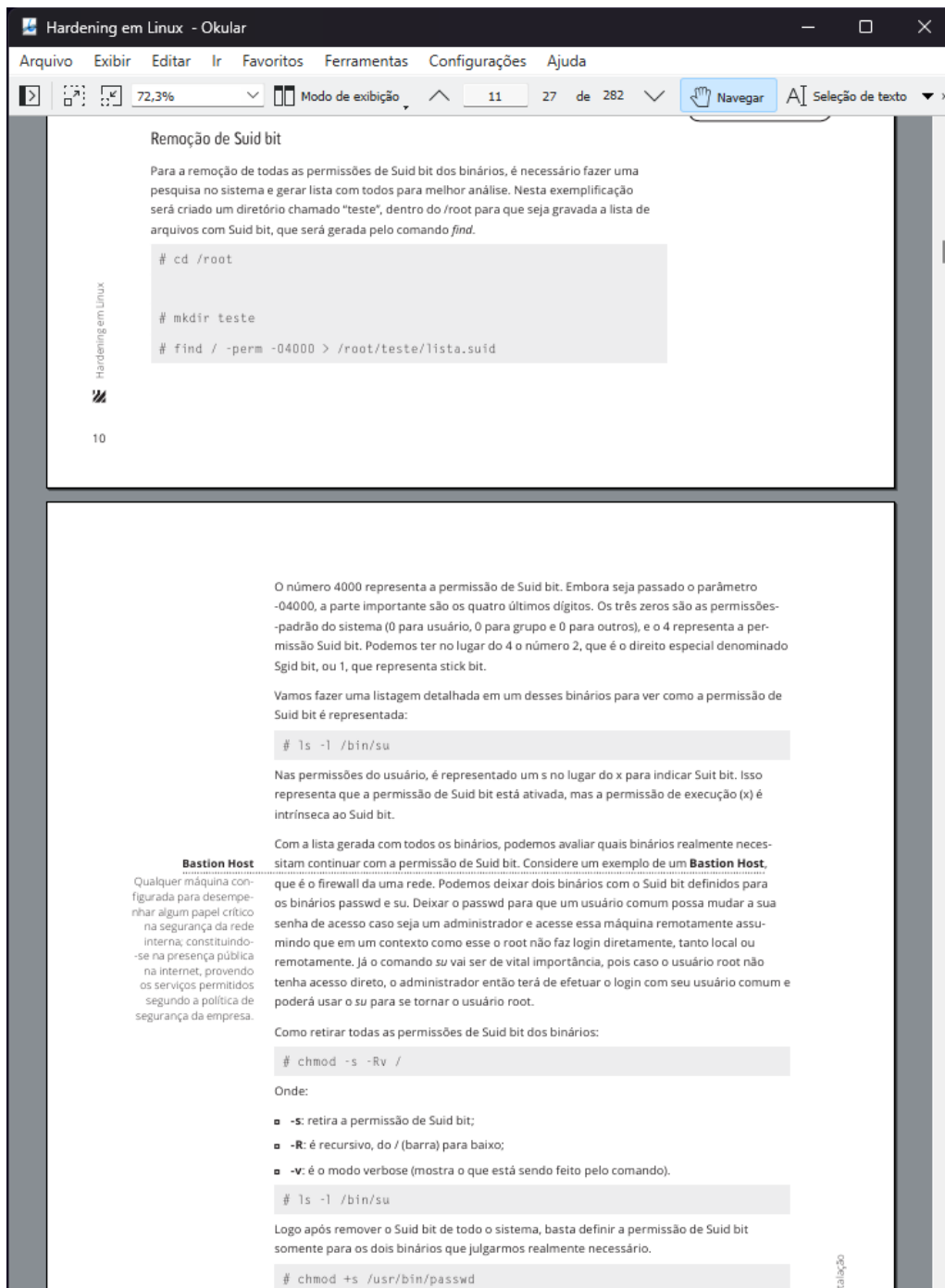
Consultar um livro requer um certo esforço e tempo, porém oferece uma abordagem estruturada e detalhada que pode se obter informações, e geralmente são escritos por especialistas no assunto, e as vezes passam por revisões e edições antes de ser publicado, que bem provável a garantia de um conteúdo confiável. Já a utilização da tecnologia do modelo de linguagem IA, como o Chat GPT, que tem grandes quantidades de texto para poder fornecer informações com respostas que podem variar em termos de exatidão e qualidade, porém depende do nível de conhecimento do usuário em relação ao tipo de consulta e da forma em que é realizada.

Devido ao surgimento exponencial de ameaças cibernéticas cada vez mais complexas, como tecnologias avançadas de IA, no caso deste estudo o ChatGPT, torna-se se um grande aliado para proporcionar uma vantagem extremamente significativa que pode colaborar com os esforços dessas ameaças. (STACK DIARY, 2023).

3. Metodologia

Um exemplo de consulta realizada em um livro conforme Figura 1 e 2, pode comprovar o procedimento de remoção de bit SUID. Quando ativo em algum arquivo, permite que o usuário execute temporariamente e assume os privilégios do proprietário do arquivo.

Figura 1 – Remoção Suid bit consultando livro



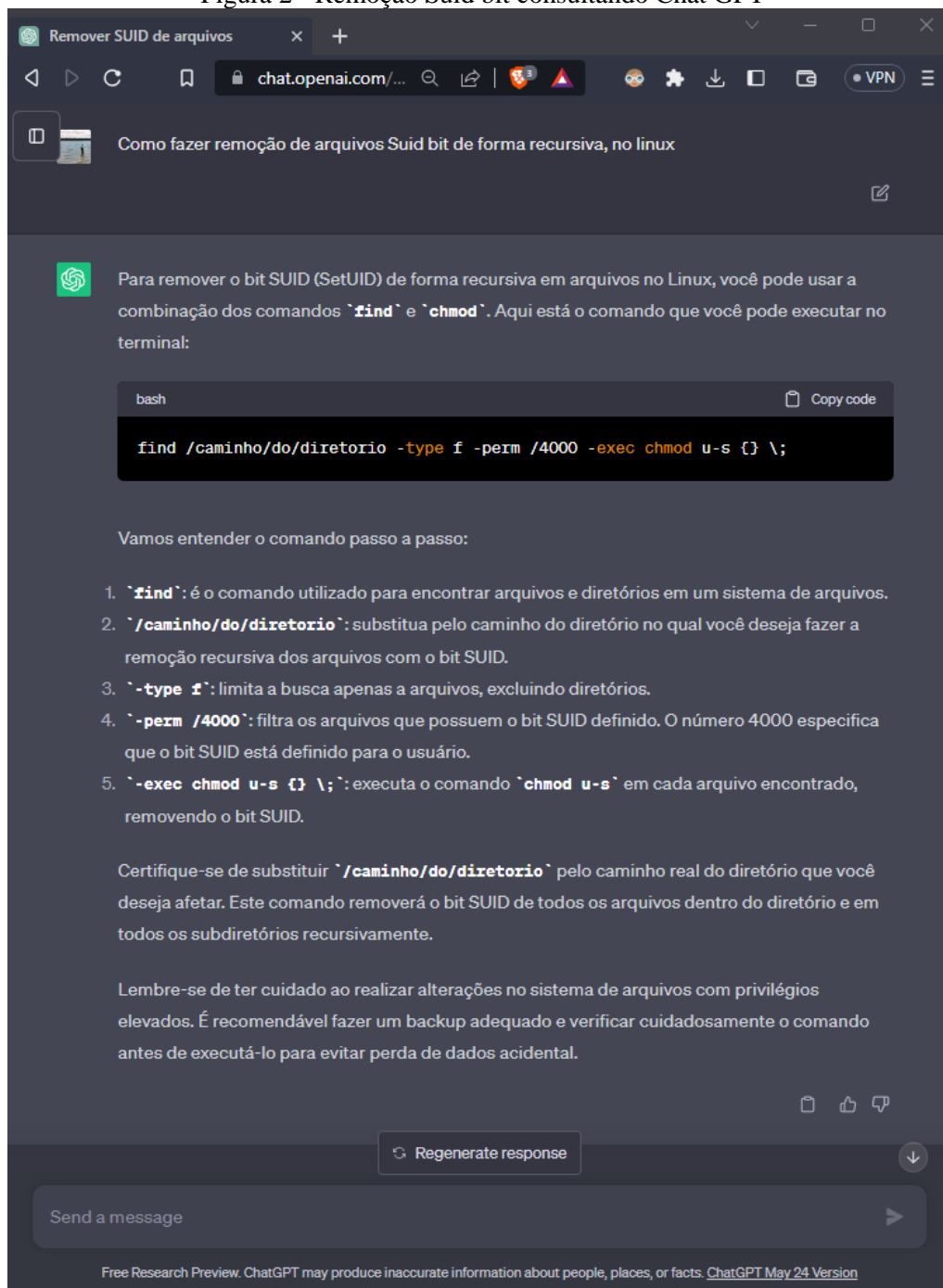
Fonte: MELO, Sandro. Hardening em Linux. RNP/ESR, 2014.

A permissão Suid bit permite que binários sejam executados com os privilégios do dono, geralmente o root. É comum em binários como 'su', 'ping' e 'passwd', mas deve ser avaliada sua necessidade. A remoção segue políticas de acesso e hardening, feita com `chmod -s -Rv /`, reatribuindo apenas a binários essenciais. 'sudo' é uma alternativa para privilégios temporários.

Já na Figura 2, é demonstrado um procedimento com uma análise um pouco mais detalhada em que um modelo de linguagem que recebe treinamento com grande quantidade de

texto para fornecer as informações, nem sempre com qualidade, porém capaz de gerar uma resposta mais instantânea, dependendo do conhecimento de quem esteja buscando essa informação talvez seja necessário consultar fontes mais confiáveis ou fazer testes em ambientes que não sejam de produção.

Figura 2 - Remoção Suid bit consultando Chat GPT



Remover SUID de arquivos

chat.openai.com/...

Como fazer remoção de arquivos Suid bit de forma recursiva, no linux

Para remover o bit SUID (SetUID) de forma recursiva em arquivos no Linux, você pode usar a combinação dos comandos `find` e `chmod`. Aqui está o comando que você pode executar no terminal:

```
bash find /caminho/do/diretorio -type f -perm /4000 -exec chmod u-s {} \;
```

Vamos entender o comando passo a passo:

1. `find`: é o comando utilizado para encontrar arquivos e diretórios em um sistema de arquivos.
2. `/caminho/do/diretorio`: substitua pelo caminho do diretório no qual você deseja fazer a remoção recursiva dos arquivos com o bit SUID.
3. `-type f`: limita a busca apenas a arquivos, excluindo diretórios.
4. `-perm /4000`: filtra os arquivos que possuem o bit SUID definido. O número 4000 especifica que o bit SUID está definido para o usuário.
5. `-exec chmod u-s {} \;`: executa o comando `chmod u-s` em cada arquivo encontrado, removendo o bit SUID.

Certifique-se de substituir `/caminho/do/diretorio` pelo caminho real do diretório que você deseja afetar. Este comando removerá o bit SUID de todos os arquivos dentro do diretório e em todos os subdiretórios recursivamente.

Lembre-se de ter cuidado ao realizar alterações no sistema de arquivos com privilégios elevados. É recomendável fazer um backup adequado e verificar cuidadosamente o comando antes de executá-lo para evitar perda de dados acidental.

Regenerate response

Send a message

Free Research Preview. ChatGPT may produce inaccurate information about people, places, or facts. ChatGPT May 24 Version

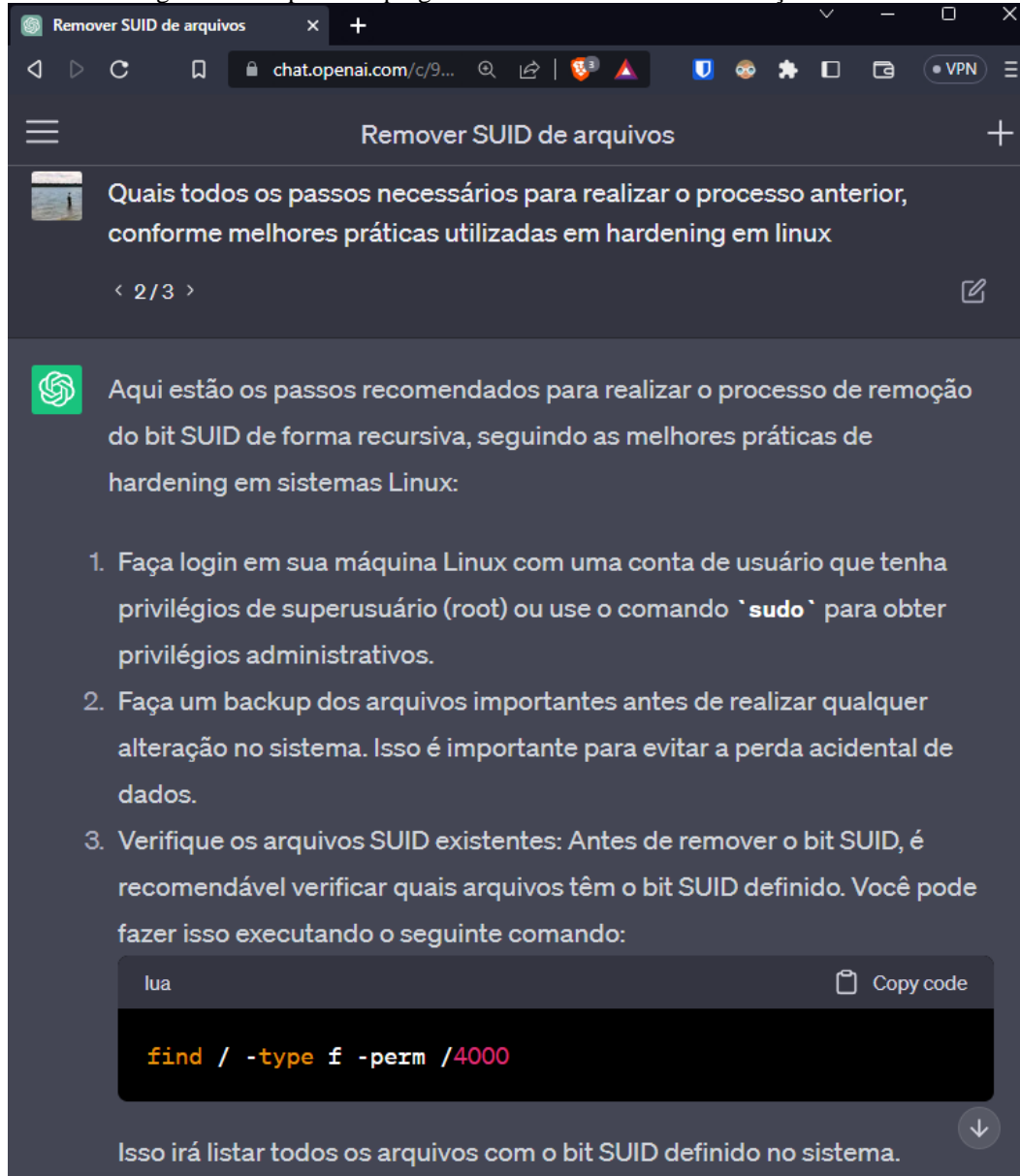
Fonte: <https://chat.openai.com/>

Em caso de insistir em uma pergunta para o Chat GPT, pode começar a retornar respostas mais detalhadas e um pouco mais informativas, dependendo do nível da pergunta, algumas das respostas podem as vezes até assemelhar às explicações encontradas no livro. Dessa forma pode

se obter respostas abrangentes e até mais assertivas, se o usuário que esteja realizando a busca tenha um conhecimento mais avançado, talvez já tenha tirado a dúvida nessa simples busca. Por tanto quanto mais rebuscada for a pergunta, mais detalhes podem ser retornados em meio as respostas.

Conforme demonstrado figura 3 e 4, a pesquisa foi realizada de maneira mais abrangente, identificando etapas adicionais que são conhecidas como boas práticas a serem adotadas durante os processos de fortalecimento da segurança.

Figura 3 - Resposta de pergunta mais detalhada sobre remoção Suid bit



The screenshot shows a chat window titled "Remover SUID de arquivos" on the OpenAI chat interface. The user's question is: "Quais todos os passos necessários para realizar o processo anterior, conforme melhores práticas utilizadas em hardening em linux". The AI response provides a list of three recommended steps for removing SUID bits recursively, following Linux hardening best practices:

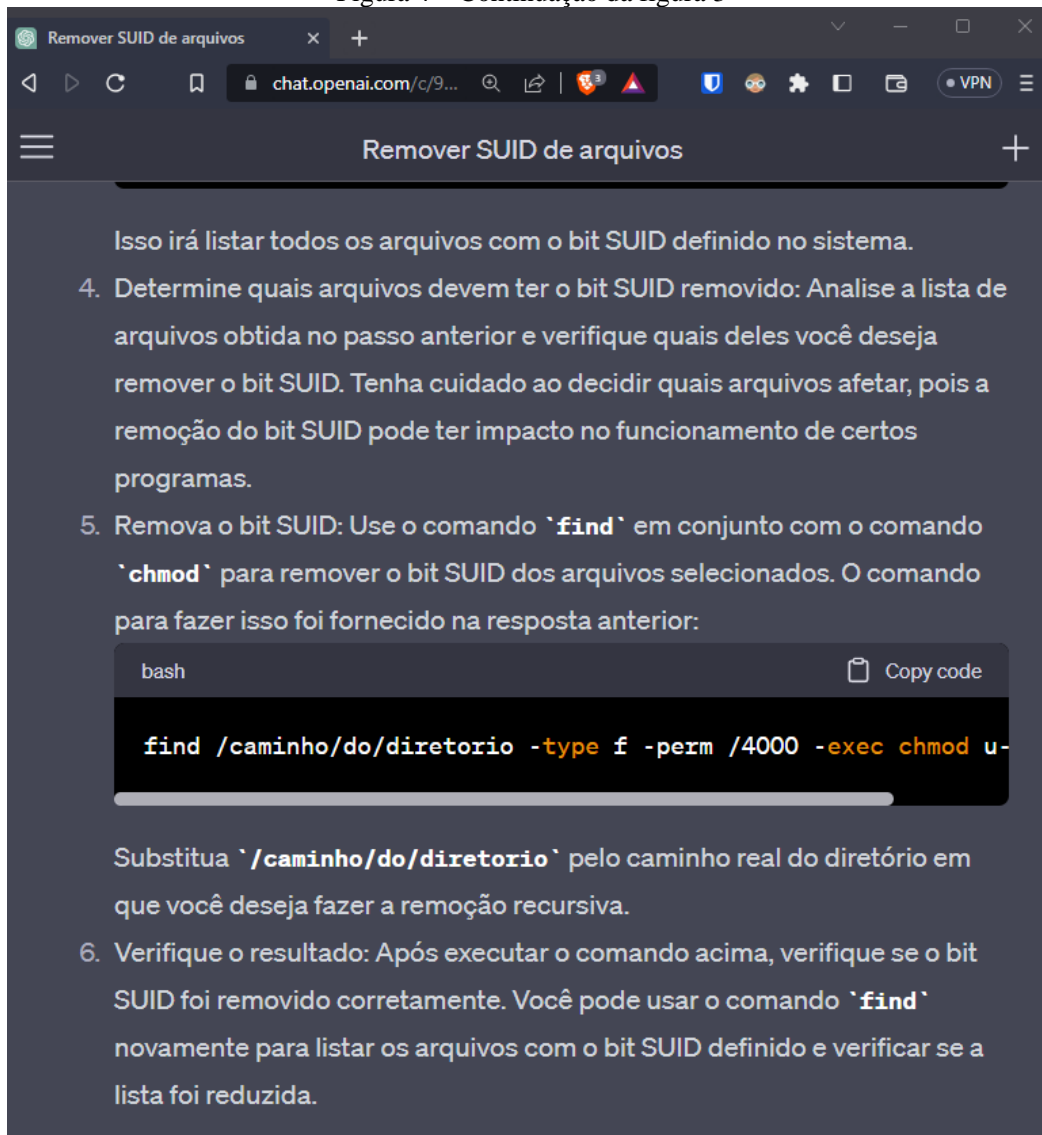
1. Faça login em sua máquina Linux com uma conta de usuário que tenha privilégios de superusuário (root) ou use o comando ``sudo`` para obter privilégios administrativos.
2. Faça um backup dos arquivos importantes antes de realizar qualquer alteração no sistema. Isso é importante para evitar a perda acidental de dados.
3. Verifique os arquivos SUID existentes: Antes de remover o bit SUID, é recomendável verificar quais arquivos têm o bit SUID definido. Você pode fazer isso executando o seguinte comando:

```
lua  
find / -type f -perm /4000
```

Isso irá listar todos os arquivos com o bit SUID definido no sistema.

Fonte: <https://chat.openai.com/>

Figura 4 – Continuação da figura 3

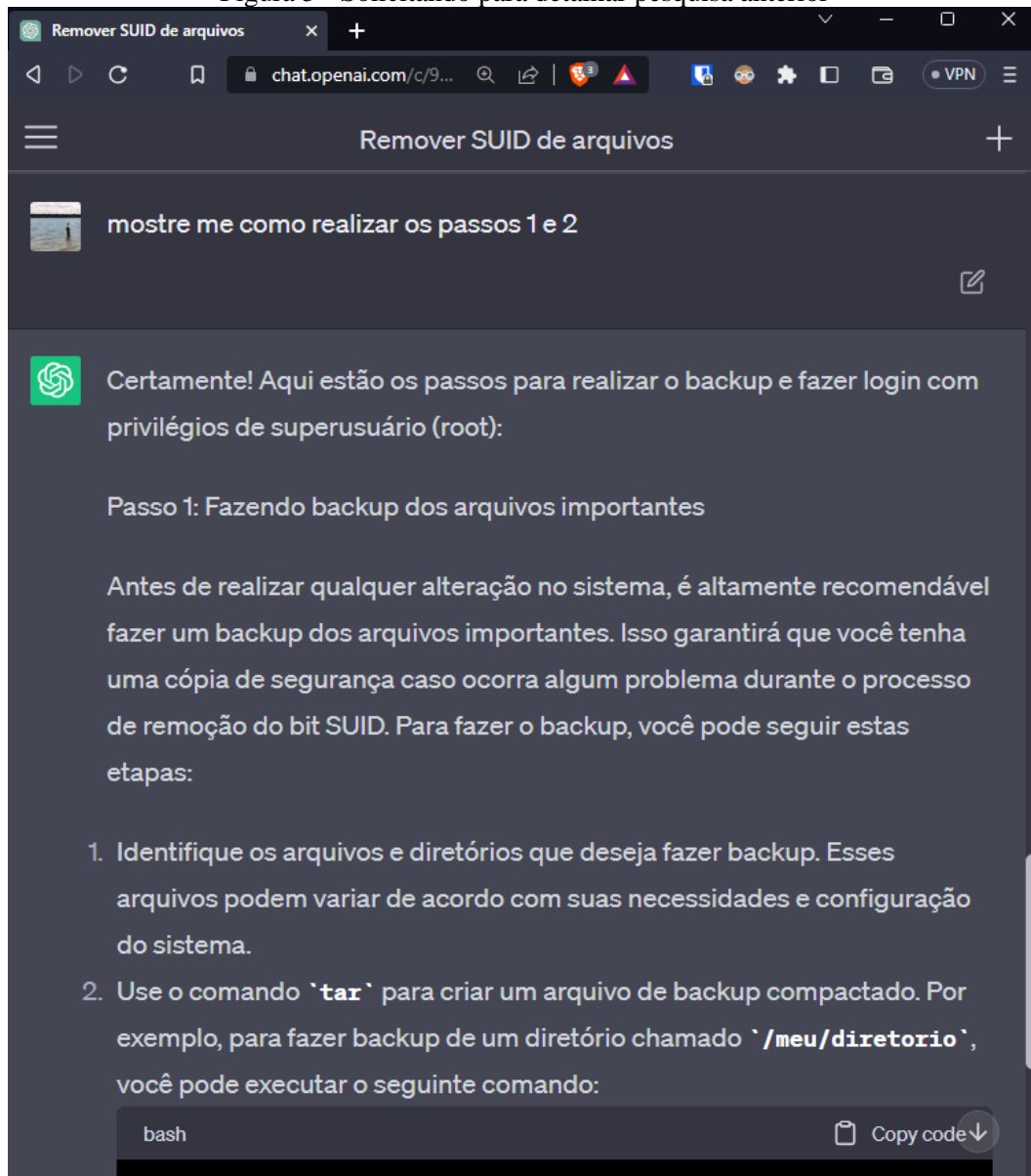


Fonte: <https://chat.openai.com/>

As Figuras 3 e 4 podem evidenciar as orientações adequadas para remover recursivamente o bit SUID em sistemas Linux. Recomenda-se fazer login como superusuário, fazer backup dos arquivos importantes, listar os arquivos com o bit SUID, escolher quais remover com cuidado e, em seguida, usar o comando "find" e "chmod" para efetuar a remoção, verificando o resultado e entendendo as possíveis implicações no funcionamento do sistema.

Caso ainda com as orientações dadas pela ferramenta de IA existam dúvidas, outra opção seria, por exemplo, questionar a possibilidade de apresentar como poderiam ser feitos, assim como mostrado nas figuras 5 e 6. Essa abordagem permite evidenciar que, em situações em que o usuário não tem um conhecimento amplo do sistema operacional Linux, é possível seguir questionando até chegar a pontos que às vezes não são diretamente discutidos no livro. Isso amplia as possibilidades de reduzir falhas e aumentar a adoção de práticas mais adequadas para aplicar a segurança durante o fortalecimento dos sistemas.

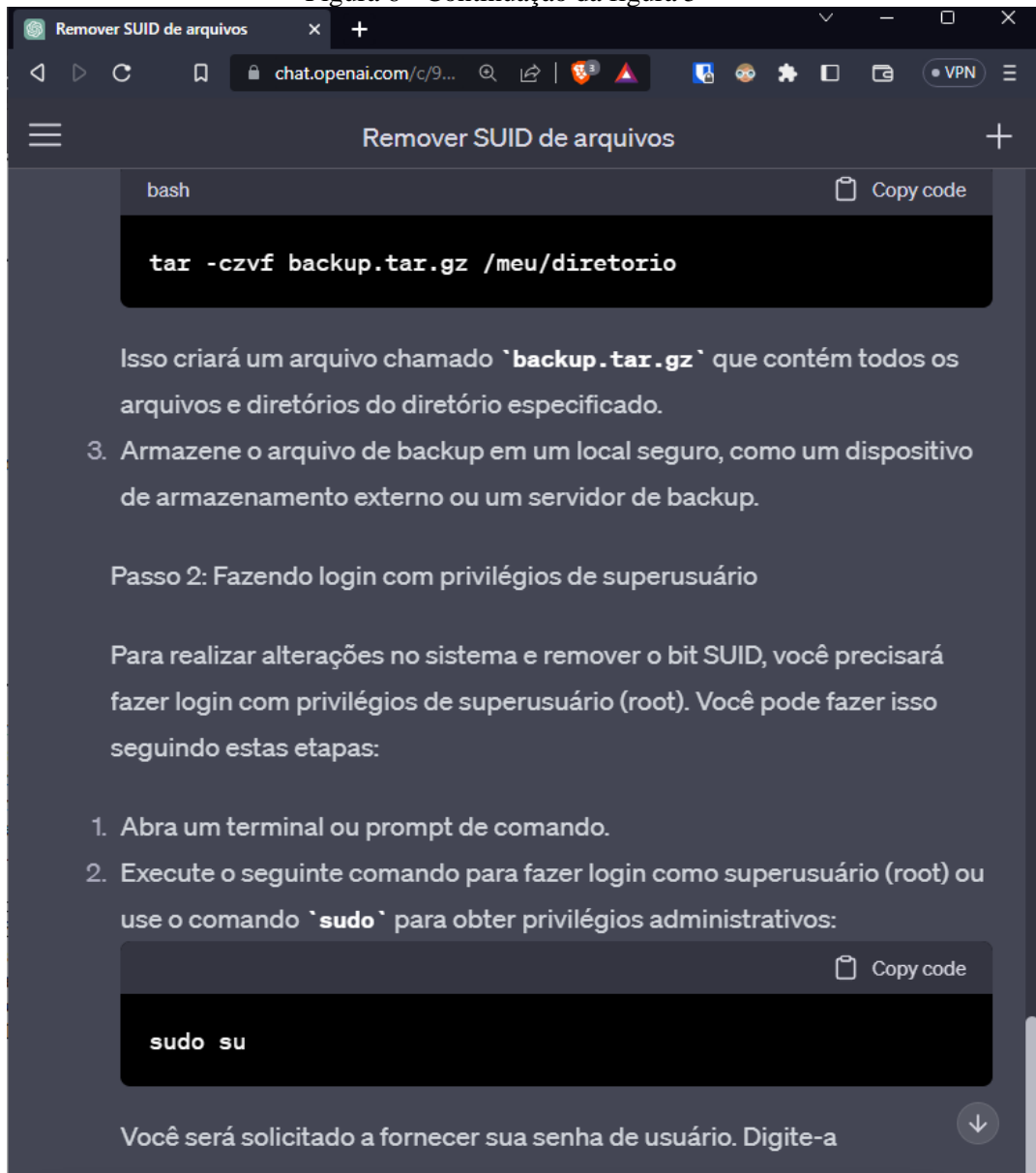
Figura 5 - Solicitando para detalhar pesquisa anterior



Fonte: <https://chat.openai.com/>

Nas Figuras 5 e 6 demonstram os passos necessários para realizar um backup de arquivos importantes e fazer login com privilégios de superusuário (root) antes de efetuar alterações no sistema, como a remoção do bit SUID. No primeiro passo, o backup é enfatizado como uma medida de segurança para garantir a preservação dos dados em caso de problemas durante as modificações. Isso é feito usando o comando "tar" para criar um arquivo compactado contendo os arquivos e diretórios selecionados. No segundo passo, é explicado como fazer login com privilégios de superusuário usando o comando "sudo su", destacando a necessidade de entender as implicações das ações realizadas com esses privilégios.

Figura 6 - Continuação da figura 5

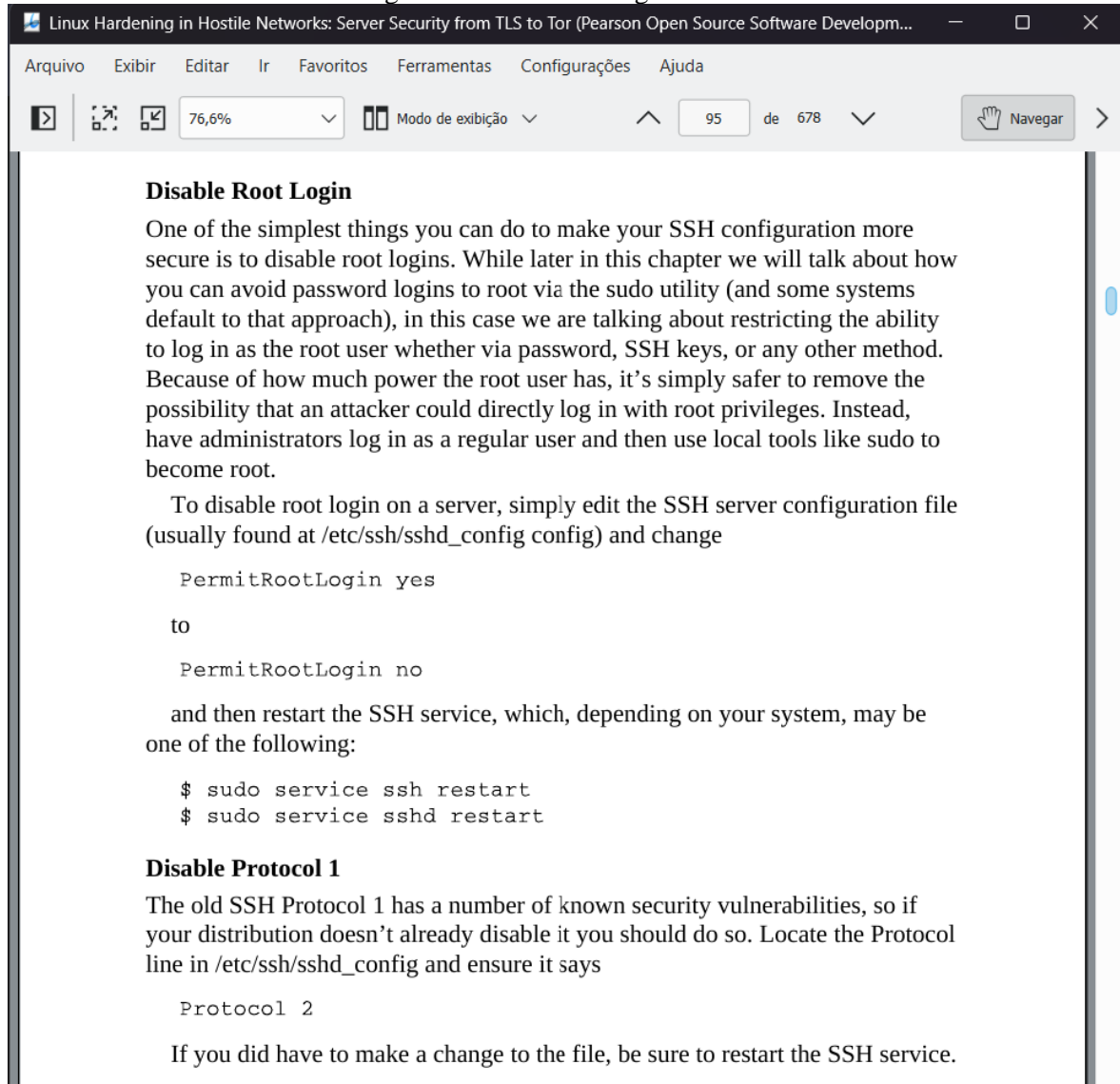


Fonte: <https://chat.openai.com/>

Como aponta Rankin (2018, p.96) com o acesso constante como usuário root ou a facilidade de acesso à conta de root pode significar conceder aos atacantes e invasores uma parte significativa do trabalho. Especialmente em ambientes corporativos, onde a distribuição da senha root é necessária para permitir que os usuários executem tarefas administrativas, surgem preocupações de segurança quando um usuário deixa a organização. Nesse cenário, é essencial alterar a senha root e distribuir a nova para evitar acesso não autorizado. Além disso, a necessidade de atribuir privilégios administrativos apenas para tarefas específicas, ao invés de conceder privilégios completos de root, é um desafio adicional. Para abordar essas preocupações, o utilitário sudo se destaca como um mecanismo eficaz no Linux e Unix, permitindo que os usuários realizem tarefas administrativas sem comprometer a segurança, mantendo apenas os privilégios necessários para a execução das respectivas tarefas.

Considerando as preocupações de acesso ao root, conforme Figura 7, o livro mostra detalhes de forma mais direta para essa configuração, mas não deixa de demonstrar amplas informações de seu processo.

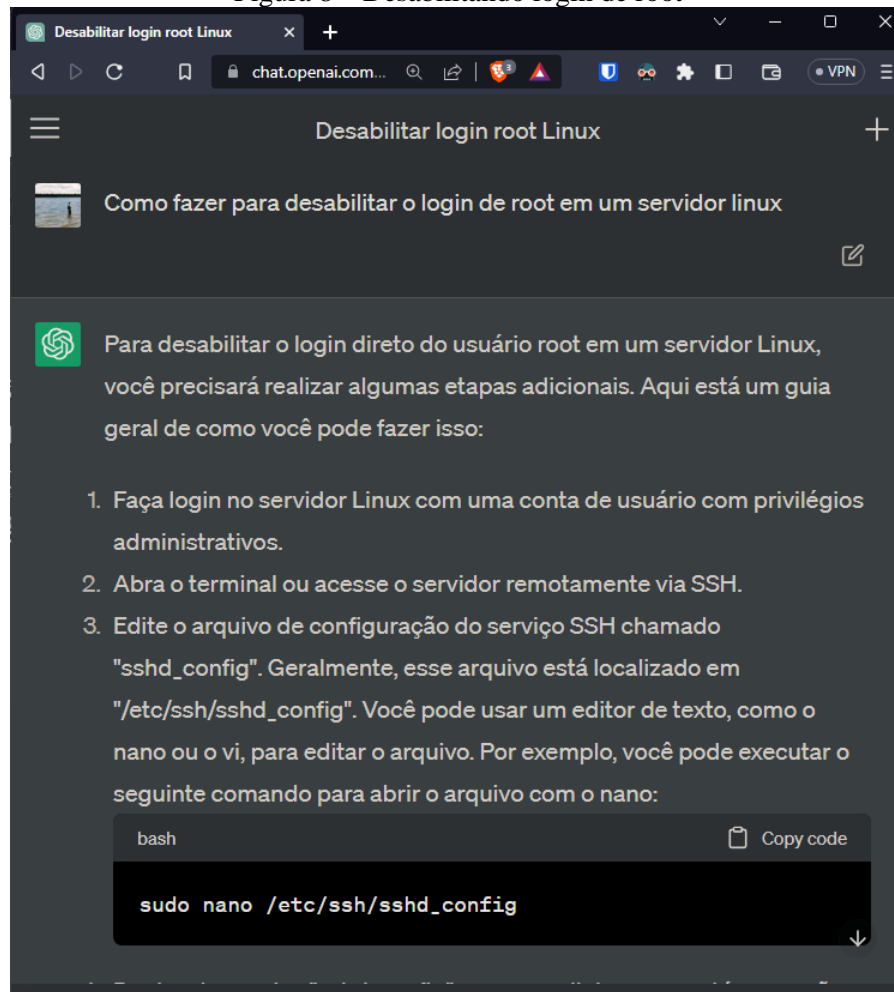
Figura 7 – Desabilitar login root



Fonte: RANKIN, Kyle. Linux Hardening in Hostile Networks: Server Security from TLS to Tor, 2018.

Conforme Figuras 8, 9 e 10 evidenciam que a pesquisa traz uma resposta praticamente igual à do livro, um tipo de guia em que mostra como desabilitar o login ao usuário root, portando demonstrando que é válido essa ferramenta, proporciona condições que possibilitam desde usuários mais experientes aos mais leigos de realizarem tarefas que possam amenizar os riscos em sistemas operacionais.

Figura 8 – Desabilitando login de root



Fonte: <https://chat.openai.com/>

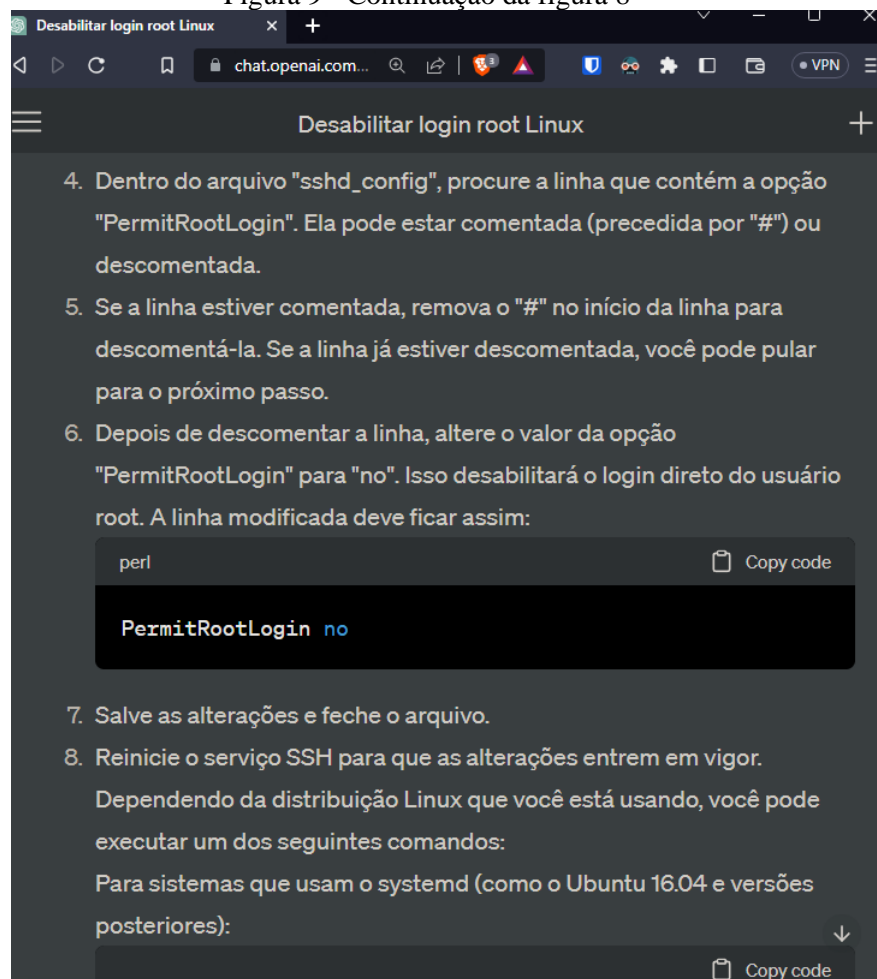
Figura 8 inicia as orientações necessárias com os seguintes passos

1 -Faça login no servidor Linux com uma conta de usuário com privilégios administrativos.

2 - Abra o terminal ou acesse o servidor via SSH.

3 - Edite o arquivo de configuração do serviço SSH chamado "sshd_config" localizado em "/etc/ssh/sshd_config" usando um editor de texto, como nano ou vi. Por exemplo, execute "sudo nano /etc/ssh/sshd_config" para abrir o arquivo com o nano.

Figura 9 - Continuação da figura 8



Fonte: <https://chat.openai.com/>

Para os passos da Figura 9, evidenciam o seguinte:

4 - No arquivo "sshd_config", encontre a linha com a opção "PermitRootLogin", que pode estar comentada ou descomentada.

5 - Se a linha estiver comentada, remova o "#" para descomentá-la; se já estiver descomentada, vá para o próximo passo.

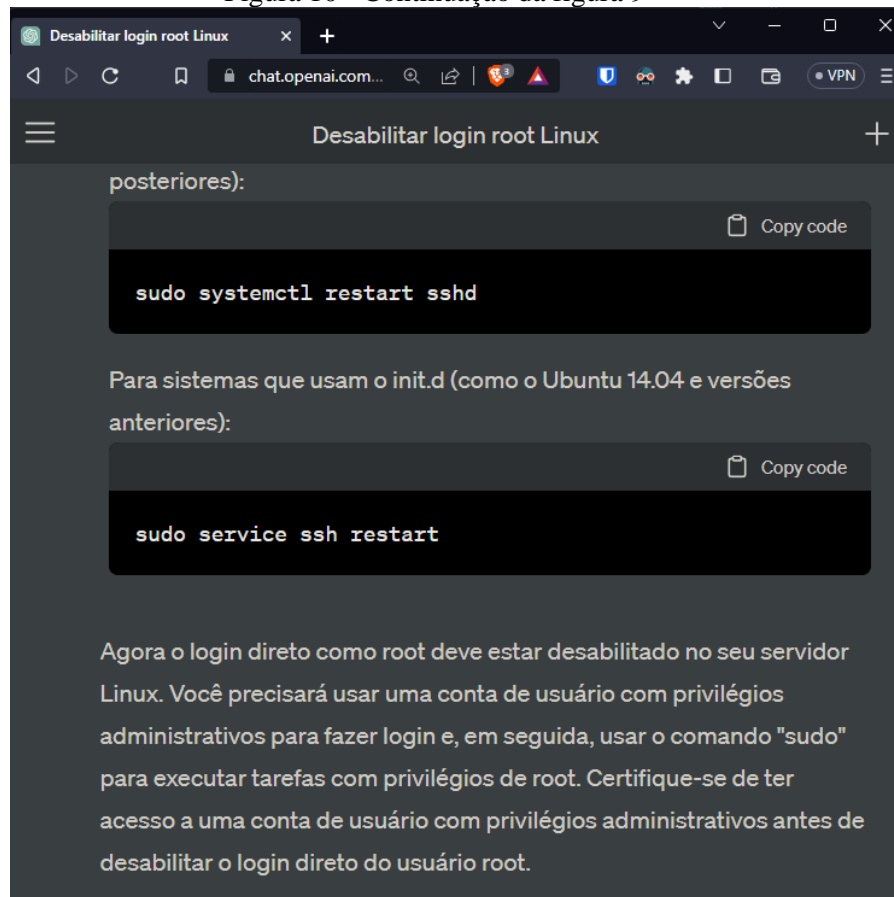
6 - Modifique o valor da opção "PermitRootLogin" para "no", desabilitando assim o login direto do usuário root.

7 - Salve as alterações e feche o arquivo.

8 - Reinicie o serviço SSH, dependendo da distribuição Linux, usando o comando apropriado, como o systemd para o Ubuntu 16.04 e versões posteriores.

O Chat GPT, um chatbot, treinado em redes neurais de aprendizado profundo para responder perguntas dos usuários. Ele utiliza processamento de linguagem natural e aprendizado de máquina para gerar respostas relevantes. Embora avançado, o algoritmo do Chat GPT pode apresentar limitações e erros em alguns contextos. Ele pode ajudar na segurança digital fornecendo informações sobre boas práticas, identificação de fraudes, sugestões de ferramentas de segurança e atualizações sobre ameaças cibernéticas. No entanto, a segurança digital é uma responsabilidade compartilhada e os usuários devem tomar medidas proativas para proteger suas informações. (ANTI HACKER APP, 2023)

Figura 10 - Continuação da figura 9



Fonte: <https://chat.openai.com/>

A Figura 10 continuar a explicação dando ênfase nos comandos para algumas versões diferentes entre o Ubuntu, como:

Para sistemas que usam o systemd (como o Ubuntu 16.04 e versões posteriores), deve-se executar o seguinte comando: `sudo systemctl restart sshd`. Isso reinicia o serviço SSH. Já para sistemas que usam o init.d (como o Ubuntu 14.04 e versões anteriores), deve-se executar o seguinte comando: `sudo service ssh restart`. Isso também reinicia o serviço SSH. E ainda orienta no final informando que após reiniciar o serviço SSH, as configurações feitas para desabilitar o login direto do usuário root entrarão em vigor. E precisará fazer login usando uma conta de usuário com privilégios administrativos e, em seguida, usar o comando "sudo" para executar tarefas com privilégios de root. Sendo necessário ter acesso a uma conta de usuário com privilégios administrativos antes de desabilitar o login direto do usuário root.

4. Discussões e Conclusão

O uso do hardening na configuração da segurança dos sistemas operacionais é de extrema importância para proteger as informações e evitar vulnerabilidades que possam ser exploradas por ataques cibernéticos. O hardening refere-se ao processo de fortalecimento do sistema, por meio da implementação de configurações preventivas e boas práticas de segurança. Ao aplicar o hardening, é possível reduzir as possíveis vulnerabilidades que um sistema pode apresentar. Isso envolve a modificação de configurações padrão, remoção de serviços desnecessários, aplicação de atualizações e correções de segurança, restrição de

permissões de acesso, entre outras medidas. O objetivo é tornar o sistema mais resistente a ataques, dificultando o acesso não autorizado e minimizando os riscos de comprometimento da segurança.

A configuração adequada do hardening pode ajudar a prevenir ataques comuns, como exploração de brechas de segurança, injeção de código malicioso, acesso não autorizado e execução de privilégios elevados.

Na questão de utilização de livros para pesquisa oferece uma abordagem estruturada e detalhada, fornecendo informações confiáveis escritas por especialistas no assunto. No entanto, requer esforço e tempo para consultar e compreender essas informações. Por outro lado, o uso da ferramenta de IA, como o Chat GPT, oferece respostas mais rápidas, embora sua exatidão e qualidade possam variar dependendo do conhecimento do usuário e da forma como a consulta é realizada.

A pesquisa demonstrou que o Chat GPT pode gerar respostas instantâneas, mas nem sempre com a mesma qualidade e detalhamento encontrados nos livros. Portanto, é recomendável que consultas mais complexas sejam complementadas com fontes mais confiáveis ou testes em ambientes não produtivos. No entanto, ao questionar o Chat GPT de maneira mais abrangente e detalhada, é possível obter respostas mais informativas e até mesmo semelhantes às explicações encontradas nos livros. Isso mostra que a ferramenta pode ser útil para fornecer informações abrangentes e assertivas, especialmente para usuários com conhecimento avançado.

Além disso, a abordagem de questionamento contínuo ao Chat GPT permite explorar aspectos que podem não ser diretamente discutidos nos livros, ampliando as possibilidades de aplicação de práticas adequadas de segurança.

Enquanto os livros oferecem informações estruturadas e confiáveis, a ferramenta de IA, como o Chat GPT, pode fornecer respostas rápidas e abrangentes, complementando o conhecimento adquirido por meio da pesquisa em livros. Ambas as abordagens têm suas vantagens e desvantagens, e a escolha entre elas dependerá das necessidades e do nível de conhecimento do usuário. Recomenda-se combinar o uso de ambas as fontes para obter resultados mais completos e confiáveis em pesquisas e estudos.

Referências

ANTI HACKER APP. Perguntas de Segurança Digital Feitas para a IA do Chat GPT. Disponível em: <https://www.antihackerapp.com.br/blog/perguntas-de-seguran%C3%A7a-digital-feitas-para-a-ia-do-chat-gpt>. Acesso em: 6 jul. 2023.

MELO, Sandro. Hardening em Linux. Rio de Janeiro: RNP/ESR, 2014. 278 p. ISBN 978-85-63630-27-8.

RANKIN, Kyle. (2018). Linux Hardening in Hostile Networks: Server Security from TLS to Tor. Pearson Education, Inc.

STACK DIARY. ChatGPT. Cybersecurity. Disponível em: <https://stackdiary.com/chatgpt/cybersecurity/>. Acesso em: 29 jul. 2023.

TOMA, Henrique E. Marie Curie. Radioatividade e era nuclear. Disponível em: https://midia.atp.usp.br/impressos/lic/modulo02/evolucao_PLC0014/evolucao_top09.pdf. Acesso em: 24 jun. 2023.